UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/775,900	02/02/2001	Martine Lapere	1585/A20	8172

2101 7590 07/28/2004

BROMBERG & SUNSTEIN LLP
125 SUMMER STREET
BOSTON, MA 02110-1618

EXAMINER	
HOFFMAN, BRANDON S	

ART UNIT	PAPER NUMBER
2136	6

DATE MAILED: 07/28/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/775,900	LAPERE ET AL.	
	Examiner	Art Unit	
	Brandon Hoffman	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-6 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-6 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 02 February 2001 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over Matyas, Jr. et al. (U.S. Patent No. 6,687,375) in view of Hoffman et al. (U.S. Patent No. 6,366,682).

Regarding claim 1, Matyas, Jr. et al. teaches a method of providing a secure transaction key, the method comprising:

- Providing a transaction key generator having an internal-key biometric input arrangement, for storing a password derived from the biometric input, and for generating a transaction code based on a transaction input, a biometric input, and the internal key (fig. 2, ref. num 56 and fig. 3, ref. num 102 and 104); and
- Deriving a personal key based on the internal key and a biometric input, and transferring the personal key to a server in a secure initialization session (figs. 4-6).

Matyas, Jr. et al. does not teach using the transaction key generator to derive a transaction code for each transaction that is communicated to the server at the time when transaction parameters are transmitted to the server; and at the server level, using the transaction parameters and the personal key to generate a reference that is compared with the transaction code to authenticate the transaction.

Hoffman et al. teaches using the transaction key generator to derive a transaction code for each transaction that is communicated to the server at the time when transaction parameters are transmitted to the server (fig. 11); and at the server level, using the transaction parameters and the personal key to generate a reference that is compared with the transaction code to authenticate the transaction (fig. 12).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine using the transaction key generator to derive a transaction code for each transaction that is communicated to the server at the time when transaction parameters are transmitted to the server; and at the server level, using the transaction parameters and the personal key to generate a reference that is compared with the transaction code to authenticate the transaction, as taught by Hoffman et al., with the method of Matyas, Jr. et al. It would have been obvious for such modifications because as is known in the art, every time a user presents his token to a device (i.e., an ATM card to an ATM machine), protection of the data needs to take place. By deriving a transaction code for each and every transaction, the user is guaranteed a safe transaction.

Claims 2-5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hoffman et al. (U.S. Patent No. 6,366,682) in view of Matyas, Jr. et al. (U.S. Patent No. 6,687,375).

Regarding claim 2, Hoffman et al. teaches a method of providing a secure authentication code from a network client to a network server, the method comprising:

- Prompting a user to provide a biometric input (fig. 3, ref. num 13);
- Decrypting an encrypted biometric token representative of a biometric input from an authorized user (fig. 8);
- Correlating the biometric input with the decrypted biometric token (fig. 12);
- Processing the authorization token to generate an encrypted authorization code (fig. 9); and
- Forwarding the encrypted authorization code to the network server (fig. 3, ref. num 1 and 19).

Hoffman et al. does not teach when the biometric input correlates to within a selected threshold of the decrypted biometric token, cryptographically transforming the biometric token to generate an authorized token.

Matyas, Jr. et al. teaches when the biometric input correlates to within a selected threshold of the decrypted biometric token, cryptographically transforming the biometric token to generate an authorized token (figs. 4-6).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine when the biometric input correlates to within a selected threshold of the decrypted biometric token, cryptographically transforming the biometric token to generate and authorized token, as taught by Matyas, Jr. et al., with the method of Hoffman et al. It would have been obvious for such modifications because the authorized token is guaranteed to be distinct for each and every user. Although the possibility is small, biometric data could be similar in some instances. A cryptographic transform of the biometric data ensures varying data between similar biometric inputs.

Regarding claim 3, the combination of Hoffman et al. in view of Matyas, Jr. et al. teaches wherein the biometric input is a spoken phrase, and the biometric token is a representation of the spoken phrase from an authorized user (see col. 1, lines 36-42 of Matyas, Jr. et al.).

Regarding claim 4, the combination of Hoffman et al. in view of Matyas, Jr. et al. teaches wherein the biometric token is encrypted and decrypted with a cryptographic key representing selected bits of a larger Data Encryption Standard (DES) key (see col. 10, lines 61-64 of Matyas et al.).

Regarding claim 5, the combination of Hoffman et al. in view of Matyas, Jr. et al. teaches wherein cryptographically transforming the biometric token includes:

- Processing the biometric token with a first transforming key representing selected bits of the DES key to produce a first intermediate token (see col. 11, lines 50-52 of Matyas, Jr. et al.);
- Processing the first intermediate token with a second transforming key representing selected bits of the DES key to produce a second intermediate token, the second transforming key being different from the first transforming key (Matyas, Jr. et al. shows providing one intermediate token which is processed with the first key to produce an authorization token. It would have been obvious to simply add a second key to apply to the intermediate token to produce a second intermediate token to create an even more secure authorization token.); and
- Processing the second intermediate token with the first transforming key to produce the authorization token (see col. 11, lines 52-56 of Matyas, Jr. et al.).

Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hoffman et al. (USPN '682) in view of Matyas, Jr. et al. (USPN '375), and further in view of Maxwell et al. (U.S. Patent No. 6,389,033).

Regarding claim 6, the combination of Hoffman et al. in view of Matyas, Jr. et al. teaches all the limitations of claim 2, above. However, the combination of Hoffman et al. in view of Matyas, Jr. et al. does not teach wherein correlating the biometric input with the decrypted biometric token includes adding reverb to the biometric input and the decrypted biometric token.

Maxwell et al. teaches wherein correlating the biometric input with the decrypted biometric token includes adding reverb to the biometric input and the decrypted biometric token (col. 2, lines 10-25).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine wherein correlating the biometric input with the decrypted biometric token includes adding reverb to the biometric input and the decrypted biometric token, as taught by Maxwell et al., with the method of Hoffman et al./Matyas, Jr. et al. It would have been obvious for such modifications because adding reverb in a closed-in location provides a better quality sound. The user of this method can not guarantee that the biometric voice input will be done in a concert hall, but instead, most likely in a room. With that said, it would be advantageous to increase the quality of the voice input by adding reverb so that a better sample is provided.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon Hoffman whose telephone number is 703-305-4662. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Brenda Hoff

BH

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100